# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/874,292 | 06/06/2001 | Gary Manuel Jackson | 63795-0007 | 6320 |

24633 7590 06/14/2006

HOGAN & HARTSON LLP
IP GROUP, COLUMBIA SQUARE
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004

| EXAMINER | |
|---|---|
| JACKSON, JENISE E | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2131 | |

DATE MAILED: 06/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/874,292 | JACKSON, GARY MANUEL | |
| | Examiner | Art Unit | |
| | Jenise E. Jackson | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *09 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,3-12 and 16-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-12, 16-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Claim Rejections - 35 USC § 103*

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 3-12, 16-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lyle et al.(6,971,028) in view of Botros et al(6,769,066).

3. As per claims 1, 30-31, Lyle et al. discloses a method for detecting unauthorized intrusion in a network system(see col. 2, lines 59-60), receiving packet level activity information from the network(see col. 2, lines 47-50, col. 10, lines 38-43); collecting sequential samples of sorted port specific activity information from the received packet level activity information for each IP/user(see col. 7, lines 3-16), converting packet level activity into human behaviors and activities for each IP/user(see col. 7, lines 32-38, 43-50), converting the sorted IP/user behavioral activities into behavioral measures of expertise and deception as measures of underlying intent for each IP/user(see col. 7, lines 43-61), monitoring sequential determinations of the converted human intent behavioral measures, for the duration that each IP/user is in the network(see col. 8, lines 34-53); wherein the monitoring step includes determining new and previously undetected misuse behaviors as indicated by increased intent levels of expertise and deception(see col. 14, lines 3-20); passive gathering of tracked intent information for any given IP/user if monitored expertise and deception measures exceed intent thresholds underlying non-misuse network activity(see col. 10, lines 38-53). Lyle et al. does not disclose identifying presence of at least

one activity, assigning a binary representation 1 to indicate present, zero to indicate absent to the at least one identified activity, generating an assessment based upon the binary rating. Botros et al. discloses identifying presence of at least one activity(see col. 6, lines 53-58), assigning a binary representation 1 to indicate present, zero to indicate absent to the at least one identified activity(see col. 10, lines 42-48); generating an assessment based upon the binary rating(see col. 10, lines 40-43). It would have been obvious to one of ordinary skill in the art at the time of the invention to include identifying presence of at least one activity and assigning a binary representation to the activity of Botros et al. with Lyle, the motivation is that by identifying and assessing a binary rating using a histogram of Botoros shows the feature values of all users over a predetermined period of time(see col. 11, lines 35-38).

4. Same motivation as above. As per claim 3, Botros et al. discloses wherein the step of generating an assessment includes associating the binary rating with an assessment based upon predetermined criteria(see col. 7, lines 1-67, col. 8, lines 1-40).

5. As per claims 4, 21, Botros et al. discloses wherein the step of generating an assessment includes mapping the assessment on at least one two-dimensional grid(see col. 11, lines 52-66, col. 12, lines 8-25). The motivation is that a histogram graph shows the distribution of a feature values for a selected feature for all users over a predetermined period of time(see Botros, col. 11, lines 36-38).

6. Same Motivation. As per claim 5, Botros et al. discloses wherein the step of mapping occurs dynamically and in real-time(see col. 10, lines 18-40).

7. As per claim 6, Botros et al. discloses wherein the step of generating an assessment includes generating a profile of the IP/user based upon the monitored behavioral measures(see

col. 7, lines 1-67, col. 8, lines 1-40). The motivation is that by generating an assessment based upon behavioral measures, one can determine whether a user's activities or normal or deviates from past behavior(see col. 9, lines 1-3).

8. As per claim 7, Botros et al. discloses wherein the step of generating an assessment is carried out utilizing a back propagation network(see col. 12, lines 45-46). The motivation is that by including the back propagation network of Botros with Lyle, is that the back propagation network includes a training algorithm that is used in network intrusion detection, to distinguish between normal behavior and anomalous behavior (see col. 12, lines 25-51 of Botros).

9. Same motivation as above(see claim 7). As per claims 8, 16, Botros et al. discloses wherein the back propagation network includes psychological assessment information (see col. 12, lines 25-51).

10. As per claim 9, Botros et al. discloses wherein the assessment is one of high deception and expertise and low deception and expertise (see col. 6, lines 53-65, col. 8, lines 46-67). The motivation is that by giving an assessment of high or low, anomalous or normal behavior can be scored accordingly (see col. 13, lines 24-41 of Botros).

11. As per claims 10, 23-24, wherein the blocking action includes sending a blocking command to a firewall for blocking further network access, Botros inherently discloses this because Botros discloses a firewall(see col. 6, lines 31-45).

12. As per claims 11, 25, Lyle et al. discloses wherein the tracking action includes storing activity information in a tracking module(see col.7, lines 13-16).

13. As per claim 26, Lyle et al. discloses wherein the tracking module includes a tracking database for storing activity information that may be used to provide evidence of an intruder's

harmful intent activities and at least one intent assessment during a session(see col. 5, lines 52-67, col. 6, lines 1-10).

14. As per claim 27, Lyle et al. discloses wherein the tracking database includes neural network assessment and associated information for the intruder that is at least one of tracked(see col. 6, lines 46-67, col. 7, lines 3-19, 32-42).

15. As per claim 28, Lyle et al. discloses wherein the tracking database includes a comparison module for comparing the neural network assessment and associated information against a second assessment based upon a second network intrusion(see col. 15, lines 45-67, col. 16, lines 1-3).

16. As per claim 29, Lyle et al. discloses tracking action is executed based upon an output from the comparison module(see col. 17, lines 40-65).

17. As per claim 12, Lyle discloses a traffic sorter that receives a copy of the network activity and sorts such all activities by IP/user for the purpose collecting sequential samples of each IP/user's activities/behaviors by IP/users(see col. 7, lines 3-12); an activity monitor operatively coupled to the traffic sorter for sequentially monitoring converted human intent behaviors and activities by IP/users(see col. 7, lines 43-58); an inter-port fusion module that fuses assessments from one or more assessment engines that monitor behavior measures by port and non-port specific behavior conversions(see col. 7, lines 43-58); and an outcome director operatively coupled to the inter-port fusion monitor(see col. 8, lines 6-14). Lyle discloses wherein the activity monitor includes at least one dedicated behavior monitor(see col. 7, lines 32-58), wherein the at least one dedicated behavior monitor includes an activity/behavior analysis module, an activity translator module and an assessment module and wherein the assessment

module(see col. 7, lines 32-64). Lyle does not disclose a trained back propagation network. Botros et al. discloses a trained back propagation network. It would have been obvious to include the back propagation network of Botros et al. with Lyle, the motivation is that by including the back propagation network of Botros with Lyle, is that the back propagation network includes a training algorithm that is used in network intrusion detection, to distinguish between normal behavior and anomalous behavior(see col. 12, lines 25-51 of Botros).

18. As per claim 13, Lyle discloses wherein the activity monitor includes at least one dedicated port monitor(see col. 7, lines 32-58).

19. As per claim 17, Lyle discloses wherein the traffic sorter receives packet level activity information from the network and sorts the port specific activity information from the network into IP users(see col. 7, lines 3-12).

20. As per claim 18, Lyle discloses wherein the activity monitor monitors the port specific activity information (see col. 7, lines 32-58).

21. See motivation as per claim 1. As per claim 19, Botros et al. discloses wherein the activity translator module assigns a binary rating based upon presence(1) or absence(0) of at least one activity/behavior detected by the packet level analysis module(see col. 8, lines 40-67).

22. As per claim 20, Botros et al. discloses wherein the assessment module generates an assessment of levels of expertise and deception present in any sample of an IP/User's overall activities/behaviors for a collection interval(see col. 6, lines 53-65, col. 8, lines 46-67). The motivation is that by giving an assessment of high or low, anomalous or normal behavior can be scored accordingly (see col. 13, lines 24-41 of Botros).

23. As per claim 22, Lyle discloses wherein an outcome director initiates a tracking command based upon the assessment result(see col. 7, lines 32-64).

24. As per claim 32, Lyle discloses wherein the step of receiving the port specific activity information includes creating a copy of the network activity sorted by users(see col. 8, lines 45-53).

25. As per claim 33, Lyle discloses the step of sorting non-port specific activity information from the received packet level activity information by the IP/user; and converting the non-port specific activity information to human behavioral measures of intent(see col. 7, lines 32-38, 43-50).

***Remarks to the Applicant***

26. Upon a more extensive review of the prior art of record, and examining the specification again, the Examiner has withdrawn the objected to material from the previous office action.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

June 9, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100